Supplement to the Final Report

Information Assurance and Information Technology:

Training, Certification, and Personnel Management in the Department of Defense

Information Assurance and Information Technology
Human Resources
Integrated Process Team

February 2000

Office of the Secretary of Defense

THIS PAGE INTENTIONALLY BLANK

Foreword

This supplement to the "Information Assurance and Information Technology: Training, Certification, and Personnel Management in the Department of Defense," was written to provide the reader with the following:

- A stand-alone description of the original report for context; and
- Updates to the original findings, recommendations, and other factors as required.

The reader should be able to gain an accurate perspective of the original findings and recommendations and the changes that occurred from the time of its release without reading the original. However, the discussions and appendicies in the original report provide valuable background for the issues and problems this Integrated Process Team addressed.

Specifically, the following sections and updates have been added to the document via this supplement:

Executive Summary:	Purpose of Supplement Significant Changes since IPT Final Report
Section 1:	Updates to Findings/Recommendations/Next Steps
Section 2:	Cost updates to Table 2

Abstract and Keywords

Abstract: The DoD's warfighting capability and the security of its information infrastructure are at great risk from attacks by foreign intelligence organizations, cyber-terrorists, and the incompetencies of some of its own users. Just as dangerous is the shortage of adequately trained and managed information technology professionals, particularly in the area of information assurance. The shortage of trained people is also critical in other parts of the public sector and in the private sector as well. In 1998, the Deputy Secretary of Defense tasked Assistant Secretary of Defense for Command, Control, Communications, and Intelligence (C3I) and the Under Secretary of Defense for Personnel and Readiness (P&R) to establish an Information Technology and Information Assurance Human Resources Integrated Process Team. This team would recommend actions, processes, and policies that would address the weakest link in DoD's defense of its information infrastructure—the people who use, administer, and manage it. The team, composed of representatives from 15 DoD organizations, concentrated on problems and issues in (1) workforce management and (2) IT and IA training and certification. In less than six months, the team developed a set of recommendations, projected results if the recommendations were implemented, cost estimates, and a five-year time line.

Keywords: Information technology (IT), information assurance (IA), Clinger-Cohen Competencies, workforce, manpower, human resources, management, weapons systems, computers, computer networks, Department of Defense, information security (INFOSEC), computer security (COMPSEC), policies and procedures.

Contents

THIS PAGE INTENTIONALLY LEFT BLANK

Tables & Charts

THIS PAGE INTENTIONALLY LEFT BLANK

Executive Summary

Purpose of Supplement

This document supplements the findings and recommendations of the Information Assurance (IA) and Information Technology (IT) Human Resources Integrated Process Team (IPT). A number of activities and events have occurred during the interim from the final work of the IPT in May 1999, the release of the report for coordination and approvals in August 1999, and the date of this re-examination. The Executive Summary and the table of recommendations are repeated here to provide a complete background for this supplement.

Purpose of IPT

This report presents the findings and recommendations of the IA/IT IPT. The Office of the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) and the Under Secretary of Defense (Personnel and Readiness) jointly commissioned the IPT in September 1998. They charged it to identify the critical IA and IT Management skill sets in the Department of Defense (DoD) and to recommend mechanisms that would promote the achievement and sustainability of those skills in the Department.

Forty-five people from fifteen DoD Services and Agencies met for the first time in late September 1998 to begin an intensive six-month analysis in response to this tasking. Their goal was to recommend actions and policies that would lead to establishing a comprehensive and world-class human resources program for IA and IT Management within the Department.

The IPT looked closely at the following areas

- Taxonomy
- Occupational descriptions and career fields
- Certification standards
- Training programs
- Accession and retention trends

Findings of IPT

Generally, there is no Department-wide recognition of the very real and growing threat to our warfighting capability as evidenced by inadequate priority, funding, training, and focus on information assurance.

The IPT's most significant finding was that IA and IT Management personnel readiness is more problematic than simply providing training opportunities and financial/career incentives to IT professionals. Before these strategies can be attempted, the Department must learn the demographics of its IT population and know precisely what IT activities it is performing already. Today, the Department is unable to expeditiously determine this information. The reasons are many, but the primary causes are that some people in non-IT career fields are performing ill-defined IA functions part time and that frequently civilian occupational series are not tied directly to IT functions. The report indicates that this fact makes it difficult to determine precisely who has access to the Department's information infrastructures. Furthermore, it makes it almost impossible to regulate training and certification requirements in what is basically a transient work force. Lastly, trying to enhance career opportunities among this unidentifiable work force is extremely difficult.

Recommendations of IPT

The IPT therefore recommends changes to the ways in which the Department manages its IT workforce. One change takes the form of recognizing specific IA functions that reflect current duties of the information age. The IPT also recommends coding IT billets and all people who perform IT functions in DoD personnel databases so that their career

progression trends and training credits can be accurately tracked. Lastly, the IPT suggests tying standardized training and certification requirements to those coded billets and people so that no one with privileged access to information infrastructures is overlooked when it comes to critical IT preparatory and sustaining education.

In four chapters and eleven appendices, the IPT report presents a strong case that the Department should take preliminary steps that will substantially improve the way we manage our IA and IT workforce. The IPT concludes that in three to five years after these recommendations are fully implemented, the Department will have the presently non-existent personnel data needed to make proper decisions concerning the creation of a career management program for IT personnel. Supporting this conclusion are nineteen distinct recommendations and associated cost estimates that—if enacted—will vastly improve the Department's IA and IT Management personnel posture.

These recommendations suggest that CINCs, Services, and Agencies adopt a consistent IA terminology and standardized Certification Criteria for certain IA functions. Recommendations further state that no one be allowed to perform these specified critical IA functions without benefit of prior training.

The recommendations also address the need for IT Management education and call for the creation of Advanced Distributed Learning programs. Equally important is the report identifies the DoD entities responsible for implementing each recommendation.

Finally, the report concludes with an implementation timeline that recognizes the major steps to complete the recommendations and the schedule for doing so. Although the timeline reflects five years for full implementation, the IPT believes that effective management and sufficient priority will result in substantive incremental progress each year, beginning with the first year.

The costs to implement these recommendations are significant in people, time, and money. If totally enacted, they will cost approximately $77.5 million over the next five years. However, the IPT is confident that the suggested course is a prudent one to position the Department appropriately in the Information Age.

The risks to our information resources are well known and the strengths of our information infrastructure defenses are being tested daily. *The weakest link in those defenses is not the technology but the people who use, administer, and manage it.* Ensuring that those people are adequately prepared for the challenge is the ultimate benefit of the IPT's work.

Significant Changes since IPT Final Report

The following events or activities provide the basis for the updates to recommendations and resources currently perceived as necessary to carry out the recommendations:

a. OPM Actions Government-wide: The Office of Personnel Management (OPM) has undertaken a government-wide piloting of new classification and qualification standards for critical IT occupations. The IA/IT IPT recommended actions support this effort.

b. ADLNet Advances in Delivery: The Advanced Distributed Learning Network (ADLNet) has made substantial progress in the development and construction of delivery mechanisms. This enables the IA/IT IPT to conclude that other organizations can focus on content development and leverage this existing and continuing investment in delivery infrastructure.

c. Reserve Components Study: Findings of a study by the Assistant Secretary of Defense for Reserve Affairs (ASD(RA)) validate many of the findings of this report, and several recommendations from this study align with the recommendations of this IPT final report and supplement.

e. Component Awareness and Training: Significant efforts have been taken by CINCs, Services and Agencies (C/S/As) to elevate awareness of the IA/IT issues through normal operations to include an increasing focus on training. These are elaborated in the update to Recommendation 18.

Table ES- 1. Recommendations and Their Priorities

Priority 1: Recommendations that have a direct impact on substantially improving the Department's ability to protect the integrity and availability of its information systems and networks and its ability to operate effectively in a joint warfighting environment.

Priority 2: Recommendations that enable the Department to substantially improve its ability to manage its IT workforce or which provide long-term efficiencies for Priority 1 recommendations.

Priority 3: Recommendations that enable the Department to improve the quality of its IT workforce and maintain improvements realized as a result of implementing Priority 1 recommendations.

Priority 4: Recommendations that will provide official policy guidance to support the recommendations above.

If the DoD Implements...	The Results Would Be...	Implementation Status
Recommendation 1: Direct the OUSD (P&R) to establish the requirement that the CINCs, Services, and Agencies identify manpower and personnel assigned IT/IA functions, enter the required information into the appropriate databases, and maintain these databases as changes occur. **(Priority 2)**	The Department's IT and IA workforces, both authorized billets and positions and personnel, will be able to be systematically and continually identified and quantified. This capability will be institutionalized.	Implementation in the mode of "business-as-usual" will require about three years once funding is provided. If sufficient priority is given to this recommendation, completion could be realized in about 18 to 24 months.
Recommendation 2: Direct the OASD (C3I) to work with the OUSD for Acquisition and Technology (A&T) and the OUSD (P&R), as part of the Inherently Governmental Working Group (IGWG), to revise IT function codes and develop definitions that more accurately reflect today's IT and IA activities. **(Priority 2)** **Recommendation 3**: Direct the OASD (C3I) to draft guidance for review by the IGWG to be used by the DoD Components to determine core IT and IA requirements to minimize the risk of losing mission capability. **(Priority 2)** **Recommendation 4**: Direct the OUSD (A&T) to consider the merits of developing and maintaining a database that shows contractor staff-years against major functions, especially IT and IA. **(Priority 4)**	The Department will have more accurate information about its government and contractor mix in the IT/IA workforce. A mechanism will be in place to maintain a core capability in these critical functions and to assess the risk of additional outsourcing.	Work is being currently initiated in these areas. By next year, information will be available to begin examination of outsourcing issues and risks.
Recommendation 5: Direct the ODASD for Military Personnel Policy (MPP) to establish a steering group comprised of OSD, Joint Staff, and each of the Services (including the Coast Guard) to focus on military IT personnel issues. **(Priority 3)**	The Department will have a forum for Services' military IT career managers to identify and assess improved methods for managing their people.	Implementation could be completed within three months or less and continue as long as the shortage of IT personnel is a serious problem.
Recommendation 6: Direct the ODASD for Civilian Personnel Policy (CPP) to work with the ASD (C3I) to widely publicize OPM flexibilities available to address civilian IT recruiting and retention problems. **(Priority 2)**	Local commanders and directors will have better information on already-approved civilian personnel management capabilities to improve their ability to recruit and retain civilian IT professionals.	Implementation can be completed within three months. The use of recruiting bonuses and retention allowances can be tracked on a regular basis.

If the DoD Implements...	The Results Would Be...	Implementation Status
Recommendation 7: Direct the OASD (C3I) to require the DoD Chief Information Officers' (CIOs) to take advantage of DoD educational programs and encourage staff personnel at the GS-13 through the GS-15 levels to complete the DoD CIO Certificate Program or the Advanced Management Program at the Information Resources Management College (IRMC). Components that wish to use information technology management (ITM) training programs other than IRMC will submit verification of equivalency to the Deputy Chief Information Officer (DCIO) office to ensure training programs cover mandatory requirements of the Clinger-Cohen Act and the Department's implementation strategies. **(Priority 3)** **Recommendation 8**: Direct the OUSD (P&R) and the OASD (C3I) to issue policy encouraging the Services/Agencies to implement a requirement that the DoD CIOs, Deputy CIOs, and Senior Executive Services (SESs) and flag officers on the CIO staffs attend DoD-sponsored ITM executive sessions or equivalent. **(Priority 3)** **Recommendation 9**: Direct the OUSD (Comptroller) to provide resources (personnel and funding) to the IRMC to accommodate additional training requirements of the DoD ITM workforce. **(Priority 3)** **Recommendation 10**: Direct the OASD (C3I) to work with the Joint Staff and the ODASD (CPP) to develop an IT contemporary issues training module for the CAP-STONE and APEX training sessions. **(Priority 2)**	Ensuring that the Department's senior executives (military and civilians) and CIO staffs are equipped with skills to effectively and efficiently make decisions regarding the development, use and management of information technologies.	CIO staff training can begin immediately. However, funding is necessary to accommodate additional throughput of students and the development of course and curricula to address new IT training requirements.
Recommendation 11: Direct the OASD (C3I) to officially adopt National Security Telecommunications and Information Systems Security Instruction (NSTISSI) Number 4009, *National Information Systems Security (INFOSEC) Glossary*, as the official IA Glossary. This requires the Defense-wide Information Assurance Program (DIAP) to formally coordinate an annex defining terminology not yet officially adopted by NSTISSI but used by the Department. **(Priority 4)** **Recommendation 12**: Direct the Joint Staff to review the defensive information operations requirements in the context of JV 2010 and translate these requirements into the Universal Joint Task List (UJTL) and the Joint Mission Essential Task List (JMETL). **(Priority 4)** **Recommendation 13**: Direct the OASD (C3I) to officially adopt the National Institute of Science and Technology (NIST) Special Publication 800-16, *Information Technology Security Training Requirements: A Role- and Performance-Based Model* and the NSTISSIs as the minimum DoD IA training standards. **(Priority 4)**	The Department will have a common IA language, a common reference point for joint training requirements, and a baseline IA training standard.	Adoption of the NSTISSI Glossary and training standards can be implemented within three months. Development of a DoD Glossary supplement and Universal Joint Task List (UJTL) and Joint Mission Essential Task List (JMETL) modifications can be implemented within six months.

If the DoD Implements...	The Results Would Be...	Implementation Status
Recommendation 14: Direct the OUSD (P&R) and the OASD (C3I) to establish the requirement that the CINCs, Services, and Agencies establish mandatory training and/or certification programs for the five "critical" IA functions, using the National Security Telecommunications and Information Systems Security Committee (NSTISSC) training standards and the IPT-developed certification requirements as the minimum requirement. In support of this, Defense Information Systems Agency (DISA) shall develop baseline IA training courses to meet the IA training requirements stipulated in the IPT certification documents. These courses can then be used by the Services and Agencies to meet the certification IA training requirement or enhanced by the Service and Agency to meet its unique needs. **(Priority 1)** **Recommendation 15**: Direct the OASD (C3I) to establish the requirement that no person assigned to a "critical" IA function at the entry level may be granted privileged access until the required IA training is successfully completed. **(Priority 1)** **Recommendation 17**: Direct the OUSD (P&R) and the OASD (C3I), in concert with the CINCs, Services, and Agencies, to coordinate biennial reviews of each certification and/or training program to ensure the currency and utility of the requirements. **(Priority 3)**	The Department will have increased assurance about the reliability of the IA workforce and its ability to protect the integrity and availability of the Department's interoperable and networked information systems. An institutionalized certification process will replace today's non-existent standards, including maintaining the currency of the standards.	Although full implementation will require three to five years once funding is provided, substantial progress can be achieved annually if appropriate priority is given to the effort.
Recommendation 16: Direct the OUSD (P&R) and the OASD (C3I) to establish the requirement that the CINCs, Services, and Agencies document these certification programs in full and develop the capability to readily produce detailed answers about the status of certifications. **(Priority 3)** **Recommendation 18**: Direct the OUSD (P&R) and the OASD (C3I) to develop and establish an Advanced Distributed Learning program, including a certification management system, for IA training and education at DISA or other appropriate location. The IA Advanced Distributed Learning effort will support implementation of an IA element within the Federal Center for Information Technology Excellence proposed under Presidential Decision Directive (PDD) 63. **(Priority 2)**	The Department will have the capability to maintain current IA training modules and deliver this training to the workforce in a timely and cost-effective manner as well as track the currency of the workforce's certification.	Although it will take five years to fully implement these recommendations, by capitalizing on similar work already completed, the requirements can be prioritized, with specific capabilities completed progressively beginning with the first year after funding is provided.
Recommendation 19: Direct the OASD (C3I) to incorporate into the DoDDIR 8500.xx, *Information Assurance*, the requirement for contractors assigned "critical" IA functions to meet the same or equivalent certification and training requirements as Department personnel. This recommendation requires that the OUSD (A&T) provide guidance to Contracting Officers to ensure these requirements are included in affected contracts. **(Priority 1)**	The Department's IT/IA contractors will meet the same minimum training and certification requirements as our military personnel and civilian employees.	The policy can be promulgated within six months. All new contracts would meet the requirements from the time the policy was promulgated. Estimates are up to two years before all existing contracts requiring changes are amended.

THIS PAGE INTENTIONALLY LEFT BLANK

1. Updates to Findings and Recommendations

1.1 Findings and Recommendations

This supplement provides updates and additional steps to implement the recommendations in the Final Report.

The key impacts of these updates and next steps are as follows:

- The cost impacts are primarily a result of savings attained by leveraging the Advanced Distributed Learning Network (ADLNet). This enables the CINCs, Services and Agencies (C/S/A's) to focus existing resources on IA training content and reduces the need for additional new resources. (See recommendation 18 update)
- The IA/IT IPT chairs conclude that the recommendations and benefits remain essentially valid as a result of at least two major actions independently undertaken since the final report and a several observations. These are the Office of Personnel Management (OPM) government-wide action (see recommendation 1 update, the initial results of a Reserve Affairs (RA) study on the abilities of the Reserve Components to assume major roles through defensive information operations and infrastructure protection missions, the increasing organizational attentiveness to IA/IT issues and subsequent focus on training (see recommendation 18 update), and the incorporation of policy recommendations in the Global Information Grid (GIG) guidance and policy memorandum (G&PM) 6-8510 and the DoD Directive 8510 on IA to replace it (see recommendation 19).

The Assistant Secretary of Defense for Reserve Affairs ASD(RA) recently undertook a study examining the Defensive Information Operations (DIO)/Information Warfare (IW) and Information Assurance (IA) capabilities of the U.S. Reserve Components to respond to cyber-terrorism and domestic terrorism in support of homeland defense. This study validated a number of the IA/IT IPT recommendations. Furthermore, several of the ASD(RA) recommendations align with the recommendations of the IA/IT IPT report.

The overall conclusion of the IA/IT IPT chairs is that the final report was correct in substance and should be approved with the changes of this supplement.

1.1.1 Finding: The CINCs, Services, and Agencies lack necessary capabilities to adequately manage the IT workforce as a whole, and the IA workforce in particular.

Recommendation 1: Direct the OUSD (P&R) to establish the requirement that the CINCs, Services, and Agencies identify manpower and personnel assigned IT/IA functions, enter the required information into the appropriate databases, and maintain these databases as changes occur. (A review is currently being conducted by the Office

of Personnel Management (OPM) of IT workforce functions to more accurately define, classify, and track IT positions and personnel. During the execution of Recommendation 1, the results of the OPM efforts can be incorporated since it will also require the identification and review of IT functions, positions, and personnel.)

This includes military, both active and Reserve components, and civilians. Modifications to existing manpower and personnel databases, as well as changes to Service/Agency directives, will be required. (Appendix G outlines the coding requirements.)

Update

CPMS recommends that OASD(C3I) be directed and coordinate with OUSD(P&R) rather than OUSD(P&R) being directed. The recommended change by CPMS is:

> **Recommendation 1**: Direct the OASD(C3I), in coordination with the OUSD(P&R), to establish the requirement that the CINCS, Services, and Agencies identify manpower and personnel assigned IT/IA functions, enter the required information into the appropriate databases, and maintain these databases as changes occur.

C3I/DCIO & DIAP: Recommend no change to original wording of recommendation 1.

Further, CPMS is investigating the cost to implement the changes to the personnel databases not covered by the services and agencies. The costs are under review with a tentative estimate of $600,000.

Air Force: Recommends no change.

C3I/DCIO: notes the following:

In an effort to improve the Government's ability to recruit and retain a well-qualified workforce in coming years, OPM has issued new classification and qualification standards for critical IT occupations. This effort is in alignment with Recommendation 1 in the IPT report. C3I/DCIO is currently participating as members of the OPM Executive Working Group in the development and review of the new specialty titles and competency-based job profiles. Two products have been designed for concurrent application and use:

- A framework of new *parenthetical specialty titles* describing IT work covered by the GS-334 Computer Specialist and GS-391 Telecommunications series.
- A *competency-based job profile* to replace the current qualification standards for the Computer Specialist and Telecommunications series.

The parenthetical specialty titles proposal includes eleven new parenthetical specialty titles for the GS-0334 Computer Specialist series. Parenthetical titles will allow for immediate recognition of current and future trends within the information technology workforce and facilitate the ability to respond to changes that may result from the continuing evolution of the occupation.

OPM developed a competency-based job profile as the new model for qualification standards that captures the full range of general and technical competencies required for IT occupations from the entry to the senior expert level. The job profile provides the competencies required for successful job performance, a description of the general and technical competencies, and a range of suggested assessment methods, to be used individually or in combination, as appropriate, for measuring an applicant's competencies.

OPM is currently soliciting agencies to participate as pilots to test the revised recruitment and classification structures. To date, the Defense Information Systems Agency is the only DoD pilot participant. The target date for completion of the pilot, finalization of the occupational structures, and classification standards is Fall 2000. Once these processes are completed and codified, agencies will be required to review positions and classify according to the new occupational categories. C3I/DCIO sees the OPM's review of the standards for the IT occupations as an opportunity to resolve several problems the Department is encountering in managing its IT workforce.

Next Steps

No substantive change to original plan of action.

1.1.2 Finding: The current trend towards outsourcing IT and IA functions raises concerns regarding potential risks to our mission.

Recommendation 2: Direct the OASD (C3I) to work with the OUSD (A&T) and the OUSD (P&R), as part of the Inherently Governmental Working Group (IGWG), to revise IT function codes and develop definitions that more accurately reflect today's IT and IA activities.

The function codes and definitions will be used by the DoD Components during the next annual Inherently Governmental and Commercial Activities Inventory.

Update

C3I/DCIO: Currently participating on the OUSD(P&R) Inherently Governmental IPT Working Group to address IT functional codes/definitions.

Next Steps

C3I/DCIO: The following are the next steps for DCIO:

- Review/analyze and compare current policies, DoD studies, current issues and debates of IT outsourcing.
- Conduct interviews with stakeholders, e.g., private industry, the Services and Defense Agencies, regarding IT functions and outsourcing.
- Interview subject matter experts in critical areas such as information assurance, architectures, and oversight to acquire input.
- Identify areas that can be outsourced with certain caveats.

- Vet resulting IT function codes along with their definitions within DoD as well as within the private sector; and address discrepancies.
- Incorporate in the OSD Inherently Governmental 2000 Reporting Inventory Guidance.

Recommendation 3: Direct the OASD (C3I) to draft guidance for review by the Inherently Governmental Working Group to be used by the DoD Components to determine core IT and IA requirements to minimize the risk of losing mission capability.

Once this core requirement has been defined and quantified, take steps to ensure that this capability is protected from outsourcing.

Update

C3I/DCIO: Developing draft of new proposed OASD(C3I) functional codes as part of the DoD inventory competitive sourcing reporting requirements. Expected completion date is March 2000.

Next Steps

C3I/DCIO: The following are the next steps for DCIO.

- Develop associated guiding principles to accompany inherently governmental reviews for IT functions.
- Incorporate guiding principles in the OSD Inherently Governmental 2000 Reporting Inventory Guidance.

Recommendation 4: Direct the OUSD (A&T) to consider the merits of developing and maintaining a database that shows contractor staff-years against major functions, especially IT and IA.

Update/Next Steps

See Recommendation 18 Update/Next Steps.

1.1.3 Finding: Each of the Services is increasingly challenged in its retention of experienced military IT personnel.

Recommendation 5: Direct the ODASD (MPP) to establish a steering group composed of OSD, Joint Staff, and each of the Services (including the Coast Guard) to focus on military IT personnel issues.

Update/Next Steps

No change.

1.1.4 Finding: The civilian personnel management and compensation flexibilities authorized by the Office of Personnel Management are not being aggressively pursued by organizations plagued with IT shortages.

Recommendation 6: Direct the ODASD (CPP) to work with the ASD (C3I) to widely publicize OPM flexibilities available to address civilian IT recruiting and retention problems.

Update/Next Steps

No change.

1.1.5 Finding: The IT educational programs offered by the Information Resources Management College (IRMC), a part of the National Defense University (NDU), are not being fully utilized by the Department to educate and train IT management professionals or functional personnel with information technology management responsibilities.

Recommendation 7: Direct the OASD (C3I) to require the staffs of the DoD CIOs at the GS-13 through the GS-15 levels to complete the DoD CIO Certificate Program or the Advanced Management Program at the IRMC. Components that wish to use ITM training programs other than IRMC will submit verification of equivalency to the DCIO office to ensure training programs cover mandatory requirements of the Clinger-Cohen Act and the Department's implementation strategies.

Update

C3I/DCIO: Recommends the following replacement of Recommendation 7's wording:

> **Recommendation 7**: Direct the OASD(C3I) to require DoD CIOs to take advantage of DoD educational programs and encourage staff personnel at the GS-13 through the GS-15 levels to complete the DoD CIO Certificate Program or the Advanced Management Program at the IRMC.

C3I/DCIO: Recommends identifying/pursuing the following initiatives to increase IRMC's annual budget to accommodate an increase in program responsibilities and additional increase in throughput of students. Toward that objective, C3I/DCIO has:

- Provided input in the DPG regarding the IRMC and IT training requirements of the Department on 11/99.
- Provided Program Budget Decision (PBD) recommendation to realign funds from within the NDU line to the IRMC on 11/99.
- Included recommendation and justification to acquire additional resources for the IRMC to support emerging requirements and increase in student throughput as part of Staffer Day briefing. (2/00)

C3I/DCIO: Recommends pursuing implementation of distance learning to accommodate additional throughput of students. Make entire CIO certificate program available via distance learning by the end of 2001. Toward this objective, C3I/DCIO has:

- Provided budget justification and detailed information regarding resource requirements for seven distance learning courses in 2000. Received partial funding to initiate conversion. To date there has been a total of 24 courses in the CIO Certificate Program. Of the courses, eight have been converted to distance learning. With 2000 funding, seven more will be brought online by the end of this fiscal year.

C3I/DCIO: Recommends drafting and coordinating a guidance memo to DoD Components outlining desired training of the CIO staffs within DoD.

- Informal discussions with the Component representatives, indicate that "desired" training of the DoD Staffs should be issued, vice "required."

Next Steps

C3I/DCIO: The following are the next steps for the DCIO:

- Draft memo with guidance regarding training/education of CIO staffs
- Meet with OUSD(P&R) staff
- Coordinate draft with Components
- Issue final guidance to Components

Recommendation 8: Direct the OUSD (P&R) and the OASD (C3I) to issue policy directing the Services/Agencies to implement a mandatory requirement that DoD CIOs, Deputy CIOs, and SESs and flag officers on the CIO staffs attend DoD-sponsored ITM executive sessions.

Update

C3I/DCIO: Recommends the following replacement of Recommendation 8's wording with the following:

> **Recommendation 8**: Direct the OUSD(P&R) and the OASD(C3I) to issue a policy encouraging the Services/Agencies to implement a requirement that DoD CIOs, Deputy CIOs, SESs and flag officers on the CIO staffs attend DoD-sponsored ITM executive sessions or equivalent annually.

Next Steps

C3I/DCIO: The following are the next steps for DCIO:

- Develop draft policy guidance outlining educational expectations of executives within DoD in regards to information technology education, training, and awareness.
- Coordinate policy memo with USD(P&R).
- Acquire comments/input from Components.

- Finalize guidance.

Recommendation 9: Direct the OUSD (Comptroller) to provide resources (personnel and funding) to the IRMC to accommodate additional training requirements of the DoD ITM workforce.

Funds will be used to execute (1) education and training initiatives outlined in this document; (2) the conversion of classroom courses to distance learning to meet the increase in throughput of students; and (3) the development of new ITM education and training requirements (e.g., development of IA Certificate Program for managers).

Update/Next Steps

No change.

1.1.6 Finding: DoD does not have a method to continuously educate and train its senior executives, military or civilian, to ensure they are equipped with the necessary knowledge and skills to make effective decisions that impact IT initiatives within their mission areas.

Recommendation 10: Direct the OASD (C3I) to work with the Joint Staff and the ODASD (CPP) to develop an IT contemporary issues training module for the CAP-STONE and APEX training sessions.

Update

C3I/DCIO: The DoD DCIO acquired input from the DoD CIO community on the critical topics that should be included in the IT training module for the CAPSTONE and APEX Programs during an offsite held in October 1999. The group agreed that there should be a two-hour IT training module addressing CIO responsibilities to support DoD missions, the Clinger-Cohen Act requirements, and CIO hot topics.

Next Steps

C3I/DCIO: The following are the next steps for DCIO:

- Work with IRMC to develop the IT contemporary issues training module as required for APEX/CAPSTONE.
- Work with the Joint Staff and Washington Headquarters Service (WHS) to incorporate/institutionalize an IT module in the CAPSTONE and APEX training sessions. Work out the details regarding the following:
  - Presenters
  - Update of materials
  - Allotment of time
  - Frequency of sessions
- Implementation of revised sessions and institution of modules programs.

1.2 IA Training: Findings and Conclusions

1.2.1 Finding: JV 2010 requirements for information superiority, coupled with the Department's interoperable systems and networks, demand a common language and common baseline of training requirements.

Recommendation 11: Direct the OASD (C3I) to officially adopt NSTISSI Number 4009, *National Information Systems Security (INFOSEC) Glossary,* as the official IA Glossary. This requires the Defense-wide Information Assurance Program (DIAP) to formally coordinate an annex defining terminology not yet officially adopted by NSTISSI but used by the Department.

Update/Next Steps

The NSTISSI is a government-wide document and is therefore applicable to DoD. The NSTISSI Working Group is re-examining the NSTISSI Number 4009. DoD has a representative to this group. The DIAP is coordinating terminology not officially adopted by NSTISSI. In particular, the GIG definitions (see Recommendation 19) are to be adopted as formal DoD definitions and include all IA terms not reflected in the NSTISSI Number 4009.

Recommendation 12: Direct the Joint Staff to review the defensive information operations requirements in the context of JV 2010 and translate these requirements into the Universal Joint Task List (UJTL) and the Joint Mission Essential Task List (JMETL).

Update/Next Steps

No change.

1.2.2 Finding: The "critical" IA functions, namely those that require privileged access, should not be assigned to the computer "hobbyist" with minimal to no formal training.

Recommendation 13: Direct the OASD (C3I) to officially adopt the NIST Special Publication 800-16, *Information Technology Security Training Requirements: A Role- and Performance-Based Model,* and the NSTISSIs as the minimum DoD IA training standards.

Update/Next Steps

No change.

Recommendation 14: Direct the OUSD (P&R) and the OASD (C3I) to establish the requirement that the CINCs, Services, and Agencies establish mandatory training and/or certification programs for the five "critical" IA functions, using the NSTISSC training standards and the IPT-developed certification requirements as the minimum requirement. In support of this, DISA shall develop baseline IA training courses to meet the IA training requirements stipulated in the IPT certification documents. These courses can then be used by the Services and Agencies to meet the certification IA

training requirement or enhanced by the Services and Agencies to meet their unique needs.

Update/Next Steps

No change.

Recommendation 15: Direct the OASD (C3I) to establish the requirement that no person assigned to a "critical" IA function at the entry level may be granted privileged access until the required IA training is successfully completed.

Update/Next Steps

No change.

Recommendation 16: Direct the OUSD (P&R) and the OASD (C3I) to establish the requirement that the CINCs, Services, and Agencies document these certification programs in full, and develop the capability to readily produce detailed answers about the status of certifications.

Update/Next Steps

No change.

Recommendation 17: Direct the OUSD (P&R) and the OASD (C3I), in concert with the CINCs, Services, and Agencies, to coordinate biennial reviews of each certification and/or training program to ensure the currency and utility of the requirements.

Update/Next Steps

No change.

1.2.3 Finding: For the most part, IA training is currently provided in a conventional classroom situation.

Recommendation 18: Direct the OUSD (P&R) and the OASD (C3I) to develop and establish an Advanced Distributed Learning program, including a certification management system, for IA training and education at DISA or other appropriate location. The IA Advanced Distributed Learning effort will support implementation of an IA element within the Federal Center for Information Technology Excellence proposed under PDD 63.

This effort must be fully integrated with the manpower, personnel, and training systems of the warfighter. The appropriate DoD, Guard and Reserve Components, and the nation's academic and training communities must be engaged in this effort. A specific program element should be established to fund development and implementation of this effort. Provisions must be included in the design of this system to ensure availability for our sea-going personnel. Web access is not always available for these personnel.

Update

The CINCs, Services, and Agencies (C/S/As) have documented their efforts throughout 1999 to address IA and IT issues. This information is also available in the larger context of IA efforts in the IA Annual Report whose descriptions are extracted below from the 1999 Annual Report.

The conclusion of this update is that the C/S/As took the findings and recommendations seriously. They have begun the process of implementing them where they can and when the resources are available. In other words, priorities on existing resources would appear to be shifting in the directions recommended by the final report. It indicates an emerging emphasis on both formal and "on-the-job" training (e.g., exercises).

Army: Emphasize classroom instruction reinforced by computer based training (CBT). Quantify the work force.

- Extensive Web based survey was undertaken in Fall 1999 to quantify Army IA workforce. Results being analyzed.
- Analysis is being done by DAMO-ODI now. Early numbers should show a large percentage of IA force is SHADOW, which is in line with the findings of the IPT. ASAM&RA will begin validations on the data collected with the major Army Commands (MACOMs) help in April.
- Different training levels were established per ASD(C3I) certification requirements. Targets soldiers, DA civilians, and contractors. The new AR 25-IA will establish certification requirements previously distributed via message.
- A database is being developed and will track all level 2 certifications. This database will be housed at the Computer Science School at Fort Gordon, GA.
- First of the additional sites for two week Systems Administrator training did pilot course in December (United States Army Reserves (USAR) and Air Systems Command (ASC)). Forts Bragg, Hood, and Lewis are targeted to come on-line by April 2000. The National Guard site should be up and running January 2000.
- Training teams were sent to field for 3 to 5 day courses; materials and ultimately lesson plans will be posted on Web.
- System administrator training in two-week resident courses at Army Computer Science School. Planning to export these courses world wide for field training. 880 certified to date.
- Courses reinforced with ARMY's enterprise- licensed CBT training.
- The Army is cooperating with several universities to establish master's and doctoral programs in information assurance.

Navy: Emphasize CNET classroom instruction and Navy Advanced Distributive Learning (Internet and computer based training). Quantify work force.

- Just-in-time training available. Pre-deployment training for BGs utilizing the Integrated Battle Force Training (IBFT) tool.

- Different training levels in accordance with ASD(C3I) certification requirements. Targets military and civilian work force. Evaluation and establishment of contractor requirements in progress.
- System administrator training and certification program. Utilization of Naval Enlisted Classification (NEC) producing schools and internet based technical training.
- SA experience time required for certification.
- Further IA courses of instruction available through various CBTs.
- The Navy is cooperating with several universities to establish college level programs in information assurance.

Air Force: Emphasize internet-based training (IBT) distant learning. Collect demographics on IBT registrants.

- IBT fielded service-wide December 1999. On annual basis, registers, trains, and tests all AF personnel and many levels of IA workforce. Produces metrics on demand. In December 1999, Air Force fielded an Air force funded ($1.2 million) centralized Information Assurance Internet-based Training system. It provides recurring distant learning IA training for all Air Force personnel (military, civilian, Guard, Reserve, and Air Force contractors).
- IA specific IBT training is provided to information systems users, system administrators and maintainers. Material includes INFOCON, basic IA responsibilities, vulnerability advisories, incident reporting, accreditation procedures, basic operating systems, and network security.
- By October CY00, IA training will be available for other network professionals (network managers, Web masters/page masters).
- Future enhancements will provide special training for information systems security organization (ISSOs), and EKMS, LRA, FORTEZZA, STE, and CAW managers and users.
- Air Force Instruction 33-115 provides overarching direction and structure for AF efforts to "Operationalize and Professionalize The Network," and promotes classroom and distant learning.

Marine Corps: Web-based registration of IT/IA workforce was undertaken in March 1999 to quantify USMC IA workforce. Collected data from military and civilian workforce with different certification levels.

- Initial IA training and awareness Mobile Team Unit sent to field in 1999. A two-hour presentation slide show with instructor/student handout/background material/references, and videos. Presentation and videos ultimately posted on Web.
- IA training presentation includes topics on threats, vulnerabilities, countermeasures, security risk, and system security plan.
- Videos includes Network at Risk, and Protect your AIS
- NETG Information System Courses- via CNET IBTs available to USMC at no cost

- USMC Computer Science School courses updated in fall 1999 - Information System Security Concept Courses- eight weeks
- INFOSEC
- Small Computer System Security
- Incident Response
- Unix Security, Windows NT Security, etc
- Defense Information Technology Security Certification and Accreditation Process (DITSCAP)
- Marine Corps General Office Networking workshop with information security/assurance modules conducted by MITRE in August 1999.

US Central Command (USCENTCOM)

- During October 1999, USCENTCOM conducted a multi-national exercise in Egypt called "BRIGHT STAR." This is currently the world's largest coalition exercise, and involved more than 38,000 U.S. and coalition soldiers, sailors, airmen, and marines. An intrusion detection system (IDS) utilizing NetRanger and Border Guard was set-up on all Tier 1 network links. The system was then monitored for suspicious activity by the 9th Information Warfare Flight (IWF) from Shaw AFB, South Carolina. The 9th IWF was able to detect probes from unauthorized sources and block these sites from performing any malicious acts. Security on the deployed network was further tested on-site by personnel from the Systems and Network Attack Center (SNAC) of the National Security Agency (NSA) and DISA FSO. DIO and IA will be incorporated into upcoming HQ exercises, such as "INTERNAL LOOK" in November 2000.

US European Command (USEUCOM)

- As part of the NSA/EUCOM Fellowship Program, two Training Needs Assessors determined USEUCOM needs in IA, relative to the duties of system administrators, information system security officers, information system security managers, and general computer users. Assessments included HQ EUCOM, United States Air Forces in Europe (USAFE), United States Army Forces, United States European Command (USAREUR), and United States Naval Forces, United States European Command (USNAVEUR), with over 80 individual interviews and 4 focus groups. The study reviewed extant courses. The result was a report detailing 18 general findings, 24 recommendations, and a detailed mapping of IA skills to specific tasks and careers ranging from military billet structures to specific training recommendations. The report also included listings of IA classes available worldwide.

US Joint Forces Command (USJFCOM)

- USJFCOM was successful in training and certifying over 3,000 users and over 100 system administrators on both the classified and unclassified networks. IA training incorporated the information contained in the DISA INFOSEC CBT CD with an instructor-led class. All new users and system administrators are trained, tested and

required to sign a letter acknowledging their appropriate roles and responsibilities for protecting the security of their systems. System administrators are required to complete Operational Information System Security CBT Volumes I and II, in addition to the DOD INFOSEC CBT.

US Pacific Command (USPACOM)

- Developed theater guidance on IA education, training, and awareness products.
- Facilitated IA training, vulnerability assessment, and certification CBT program in conjunction with OSD initiatives.
- Improved education and awareness of IA.

US Southern Command (USSOUTHCOM)

- Developed a comprehensive training program that satisfies ISSO and SA certification requirements and that enhances the overall IA posture within USSOUTHCOM. Training is accomplished through commercially produced CBT products from Learning Tree as well as contracting local vendors for training. The command wide statistics, including the system administrators at remote locations throughout the area of responsibility (AOR), for Level 1 Certification are:
  - 130 NT system administrators identified, of which 40 are certified;
  - 13 NT ISSM/ISSOs identified, of which 4 are certified;
  - 92 Unix system administrators identified, of which 29 are certified;
  - 9 Unix ISSM/ISSOs identified, of which 5 are certified;
  - sponsored 6 Unix Security courses through a local commercial vendor, with a total of 91 students trained (95%).
- Created a USSOUTHCOM-specific Information Systems Security CBT for system users. The interactive CBT incorporates a testing feature and automatic reporting to the J6 Network Security Branch for monitoring compliance with DoD policy. System users are required to pass the CBT within 30 days of their account activation and annually thereafter. User accounts are disabled for failure to complete the CBT as prescribed.
- Reinforced user awareness training through the monthly publication of *The Informer* newsletter. The newsletter focuses on relevant security issues to the command. In addition, the headquarters has an annual Computer Security Day in April. Computer security posters and promotional items emphasize the importance of using good INFOSEC practices. This year's event included an IT exposition with 15 vendors.

US Special Operations Command (USSOCOM)

- January 1999 began with the first USSOCOM IA Meeting, hosted by HQ USSOCOM with participation from the Joint Special Operations Command (JSOC) and the Service components. The purpose of these meetings was to further information sharing and training. The initial session included training provided by the IA Technology Analysis Center (IATAC) in the area of Penetration Testing. Additional training was conducted for Unix and network security, computer

forensics, and instructions on performance as a Contracting Requirements Action Officer. To help the HQ USSOCOM Staff better understand and support JSOC and the service components, a Staff Assistance visit was conducted in February 1999.

US Strategic Command (USSTRATCOM)

- A collaborative partnership between USSTRATCOM and the Peter Kiewit Institute of Information Science, Technology and Engineering was formed to meet the ever-increasing need for information technology professionals in the Omaha, Nebraska, area and around the nation. Realizing the importance of first-hand cyber-security experience, over 20 of USSTRATCOM's information technology professionals volunteered their time to personally mentor Peter Kiewit Institute students. USSTRATCOM will hire six students as interns starting in January 2000, using the OPM Student Temporary Employment Program (STEP).

US Transportation Command (USTRANSCOM)

- In 1999 USTRANSCOM continued to manage and operate a world-class information systems security program. This included development of new security policies and procedures, and development of a new, comprehensive security education, training, and awareness program.

National Security Agency (NSA)

- No change

Defense Information Systems Agency (DISA)

- The following activities have occurred since May 1999, the DISA SA Certification Program was revised on November 29, 1999 and the change includes:

  (a) Level 1 re-certification for SA's changed from 3 years to every 18 months;

  (b) Additional coursework added for re-certification is a CD - "Introduction to the Defense Information Technology Security Certification and Accreditation Process (DITSCAP)";

  (c) security CD Cyber-Protect and a CBT on Internet Security: Firewall Principles.

- Level 2 must complete all above if not already satisfied. In addition, a System Administrator Incident Preparation and Response (SAIPR) CD for Windows NT and Unix was added to the Level 2 training. And finally, a DISA definition for Level II Programs has been established, although we have none certified yet. This portion of activity has incurred no cost change as it reflects the on-going missions activities of DISA

- DISA provided IA education, training and awareness (ETA) products. This activity provided CINC, Service, and Agency personnel both classroom training and interactive multimedia CBT and awareness to support certification of system administrators and users. Products developed and disseminated by DISA/IPMO are being used in Service Schools and training organizations, by unit trainers to support

IA training and awareness in the field, and by individuals seeking to enhance their IA knowledge and skills.

- DISA ETA initiatives included: Produced Public Key Infrastructure CBT products; the CINDI Award-winning CYBERPROTECT CBT, and an innovative IA training exercise for system administrators, information system security officers and managers and other IA personnel; to support OSD mandate for DoD Certified system administrators, updated Unix Security and Windows NT Security for a system administrator classroom course and began transition to CBT; under the IPMO Franchise Program, qualified US Army Reserve trainers at Ft McCoy, Wisconsin to deliver DITSCAP and Introduction to Information System Security courses; disseminated 100,000 IA training and awareness CBTs and videos DoD and Federal-wide, up from 30,000 in FY98; in support of DoD and Federal outreach programs to industry and academia, obtained a DoD open dissemination release for most CBTs, and facilitated making the products available to the general public through the National Technical Information Service (NTIS) of the Department of Commerce; continued to facilitate integration of INFOSEC training and awareness classroom materials, videos, and CDs into Service/Agency school-house curriculums. These serve as pre-requisites to establish baseline level of knowledge prior to class, and are being used to reduced classroom time required to cover the same amount of information, or allow additional hands-on training, and/or permit addition of new material without increasing course length.

Defense Logistics Agency (DLA)

- Provided security awareness products to all DLA activities, and conducted several security awareness sessions for employees.
- Certified all system administrators responsible for SIPRNET connections, in compliance with DoD mandate.
- Conducted the first CIO IA Conference for Information System Security Officers and System Administrators. Next one is currently scheduled for March/April 2000 timeframe.
- Identified and developed associated training requirements, sources, and methods for IT/IA functions.
- Identified retention requirements.
- Implemented Deputy Secretary of Defense-required information assurance certification and training of SIPRNET system administrators and users. IA personnel are receiving minimum-security requirements

National Counterintelligence Center (NACIC/NIPC)

- Solar Sunrise: Dawn Of A New Threat - Training Video: The National Counterintelligence Center (NACIC) released a new security awareness training video entitled "Solar Sunrise: Dawn of a New Threat." The new video, 18 minutes long and produced in cooperation with the Federal Bureau of Investigation (FBI) and the National Infrastructure Protection Center (NIPC), highlights a 1998 FBI/NIPC

computer hacker investigation involving assaults on military computer systems across the country.

Next Steps

DISA: The following steps are envisioned by DISA in coordination with ADLNet:

Focus on Content

This approach relies on existing commercial-off-the-shelf (COTS) solutions for delivery. It does not attempt to advance ADL technology.

The *Department of Defense Strategic Plan for Advanced Distributed Learning* (April 30, 1999) identifies five elements needed to develop and successfully implement the ADL:

- Common industry standards (Shareable Courseware Object Reference Model (SCORM))
- Interoperable tools and content
- A robust and dynamic network infrastructure for distribution
- Supporting resources
- Cultural change at all levels of command

The DIAP recommends that the ADL continue its efforts with regard to standards. The IA ADL program will use proven COTS tools. It also will use the network infrastructure as it evolves, and assumes that the overall DoD ADL will work to influence that evolution.

Regarding supporting resources, the IA ADL program funding will support conversion of traditional classroom IA courseware to ADL media that is compliant with the ADL SCORM, as well as development of new content. Development and conversion would be in a form consistent with emerging standards of interoperability and reuse.

It also would fund the delivery of IA training and awareness content, including instructors who, regardless of the delivery mechanism, are an integral part of the training process.

Establish Partnerships

The objective here is to share common costs and promote the efficient usage of the delivery media. Working with an existing ADL enterprise delivery means/infrastructure rather than setting up a new facility may reduce some costs. Possible partners include the following:

- Defense Intelligence Agency (DIA), which is currently setting up a virtual university for the intelligence community
- USAF, which is setting up an IA distance learning capability
- CNET
- National Guard
- US Joint Forces Command

In addition, the DoD ADL Program has established several ADL Co-Labs, and there are a number of prototype programs associated with the DoD ADL community.

DIA appears eager to have others use its infrastructure to deliver training. The DIA Virtual University represents a recent real-world requirement. The estimate from the contractor who is satisfying the request is a real-world response. The total cost of the initial effort, for contractor labor only, is approximately $7 million over five years, predominantly for the transition of classroom content to distributive training media. The estimated total cost of DIA Virtual University is approximately $20 million[1]. Given the technical, hands-on nature of the training to be delivered, and the dynamic nature of the entire IA environment, the IA ADL effort is likely to require more content development and more frequent update of existing content once it is transitioned to distributive media.

Ensure Baseline IA Training Courses (R-4) Can Be Used by IA ADL Program (R-18)

Recommendation 4 provides for development of IA training content. The products developed under this recommendation could support the ADL initiative. Since the ADL recommendation is assumed to have included costs for developing and transitioning courseware, this reduces the total cost by $10.5 million (from $49 million to $38.5 million). The $10.5 million recommended by the IPT report is considered the minimum required for the development of products such as the CDs currently produced by DISA, and is assumed to be in addition to the current ~$1.5-2.0 million funding level of DISA's DoD ETA program. The Table below identifies current and proposed spending on DoD level IA training and awareness products and delivery.

	FY00 ($M)	FY01 ($M)	FY02 ($M)	FY03 ($M)	FY04 ($M)	FY05 ($M)	TOTAL ($M)
Content (R-4)		2.1	2.1	2.1	2.1	2.1	10.5
ADL (R-18) Content Delivery*		2.0	2.0	2.5	2.5	2.5	11.5
		2.0	2.4	2.6	2.8	3.0	12.8
Current DISA / IPMO IA ETA Funding**	1.8						
TOTAL	1.8	6.1	6.5	7.2	7.4	7.6	34.8**

NOTES:

* Includes cost of ADL-delivered material, plus cost of instructors necessary to support delivery. Savings are obtained not in the cost to develop, but in the cost per student to deliver. Classroom instruction may reach 500 students a year; Distributive instruction, backed by a qualified instructor / subject matter expert, may reach or more in a year, with additional savings to the Department overall from reduced student temporary duty expenses.

** This number does not take into account funding that DISA is likely to program for IA ETA. Assuming $2 million a year, the total additional funding required by DOD is approximately $25 million over five years.

[1] Another current effort, the Navy CNET Virtual University may cost as much as $120 million, but this includes all costs, not just contractor costs.

1.2.4 Finding: With an increasing contractor IA workforce, it is important to ensure that this segment of our workforce does not become the weak link in protecting our information systems. The Department must ensure that contractors are subject to the same training and certification requirements as its own personnel.

Recommendation 19: Direct the OASD (C3I) to incorporate into the DODD 8500.xx, *Information Assurance*, the requirement for contractors assigned "critical" IA functions to meet the same or equivalent certification and training requirements as Department personnel. This recommendation requires that the OUSD (A&T) provide guidance to Contracting Officers to ensure these requirements are included in affected contracts.

Update/Next Steps

Draft Global Information Grid (GIG) Guidance and Policy Memorandum (G&PM) 6-8510 on IA states that "all DoD personnel and support contractors shall be trained and appropriately certified to perform the tasks associated with their designated responsibilities for safeguarding and operating GIG information systems," and gives DoD Component Heads responsibility for ensuring that required training and certification are provided. The wording does not differentiate between "critical" IA functions and others, but has the net effect of requiring contractors to meet the same training and certification criteria as DoD employees. It is anticipated the G&PM will be signed by the end of March 2000. Similar requirements will also be included in a DoD Directive 8510 on IA that will replace the G&PM within 180 days from the signing and release of the G&PM.

2. Roadmap to Improvements

2.1 Implementing the IPT Recommendations

Previous chapters presented the IPT's recommendations. These recommendations, when fully implemented, will significantly improve the Department's capability to meet the JV 2010 goal of information superiority. What the Department will accomplish is depicted in Table 1.

Table 1. Anticipated Results and Implementation Status

If the DoD Implements...	The Results Would Be...	Projected or Current Status
Recomm. 1	The Department's IT and IA workforces, both authorized billets and positions and personnel, will be able to be systematically and continually identified and quantified. This capability will be institutionalized.	Implementation in the mode of "business-as-usual" will require about three years once funding is provided. If sufficient priority is given to this recommendation, completion could be realized in about 18 to 24 months.
Recomms. 2, 3, and 4	The Department will have more accurate information about its government and contractor mix in the IT/IA workforce. A mechanism will be in place to maintain a core capability in these critical functions and to assess the risk of additional outsourcing.	Work is being currently initiated in these areas. By next year, information will be available to begin examination of outsourcing issues and risks.
Recomm. 5	The Department will have a forum for Services' military IT career managers to identify and assess improved methods for managing their people.	Implementation could be completed within three months or less and continue as long as the shortage of IT personnel is a serious problem.
Recomm. 6	Local commanders and directors will have better information on already-approved civilian personnel management capabilities to improve their ability to recruit and retain civilian IT professionals.	Issuance of information and the Implementation of marketing strategies can be completed within three months. The use of recruiting bonuses and retention allowances can be tracked on a regular basis.
Recomms. 7, 8, 9, and 10	IT training for the Department's senior executives (military and civilians) and CIO staffs will meet the requirements of the Clinger-Cohen Act.	CIO staff training can begin immediately. However, funding is necessary to accommodate additional throughput of students and the development of course and curricula to address new IT training requirements.
Recomms. 11, 12, and 13	The Department will have a common IA language, a common reference point for	Adoption of the NSTISSI Glossary and training standards can be implemented

If the DoD Implements...	The Results Would Be...	Projected or Current Status
	joint training requirements, and a baseline IA training standard.	within three months. Development of a DoD Glossary supplement and UJTL and JMETL modifications can be implemented within six months.
Recomms. 14, 15, and 17	The Department will have increased assurance about the reliability of the IA workforce and its ability to protect the integrity and availability of the Department's interoperable and networked information systems. An institutionalized certification process will replace today's non-existent standards, including maintaining the currency of the standards.	Although full implementation will require three to five years once funding is provided, substantial progress can be achieved annually if appropriate priority is given to the effort.
Recomms. 16 and 18	The Department will have the capability to maintain current IA training modules and deliver this training to the workforce in a timely and cost-effective manner as well as track the currency of the workforce's certification.	Although it will take five years to fully implement these recommendations, by capitalizing on similar work already completed, the requirements can be prioritized, with specific capabilities completed progressively beginning with the first year after funding is provided.
Recomm. 19	The Department's IT/IA contractors will meet the same minimum training and certification requirements as our military personnel and civilian employees.	The policy can be promulgated within six months. All new contracts would meet the requirements from the time the policy was promulgated. Estimates are up to two years before all existing contracts requiring changes are amended.

2.2 Priorities

The nineteen recommendations are grouped into four priorities: 1, 2, 3, and 4.

- **Priority 1** recommendations are those which have a direct impact on substantially improving the Department's ability to protect the integrity and availability of its information systems and networks and its ability to operate effectively in a joint warfighting environment. *Recommendations 14, 15, and 19.*
- **Priority 2** recommendations are those which enable the Department to substantially improve its ability to manage its IT workforce or which provide long-term efficiencies for Priority 1 recommendations. *Recommendations 1, 2, 3, 6, 10, and 18.*
- **Priority 3** recommendations are those which enable the Department to improve the quality of its IT workforce and maintain improvements realized as a result of implementing Priority 1 recommendations. *Recommendations 5, 7, 8, 9, 16, and 17.*
- **Priority 4** recommendations are those which will provide official policy guidance to support the recommendations above. *Recommendations 4, 11, 12, and 13*

2.3 Costs

These recommendations are not without cost. The IPT's recommendations are listed in Table 2 on page 22, along with the costs to implement. Approving the recommendations will not result in implementation, simply another unfunded requirement. Appropriate dollars must be provided. To fully fund these recommendations will require $77.5 million over the next five years. Once the recommendations are approved and the dollars provided in the budget, the timelines shown in the next section can commence. See Appendix K for Service and Agency cost breakouts.

Update/Next Steps

Cost updates now indicate a total funding of $64.19 million versus $77.5 million.

2.4 Timeline for Implementation

The timeline shown in Appendix L begins with Month 0. Month 0 is defined to be that month in which implementation is directed and, when required, dollars are provided.

2.5 Future Issues to be Addressed by OSD

There are a number of issues left unresolved due to a lack of personnel data. Once Recommendation 1 is fully implemented, the workforce needs to be analyzed and management alternatives examined with respect to:

- The impact of the non-IT professional assigned IT functions;
- The size and distribution of the civilian IT professional workforce and the desirability of a career management program for that workforce; and
- Recruiting and retention statistics for the civilian IT workforce and identification of required management actions.

There are two additional issues that should be considered for additional work:

- Certification requirements should be developed for the non-critical IA functions.
- Staffing guidelines for manpower-intensive IA functions should be developed using independent variable(s) that can be easily determined during the program/budget process.

Table 2. IPT Recommendations and Their Costs

Recommendation	Page	Cost
Recommendation 1: Direct the OUSD (P&R) to establish the requirement that the CINCs, Services, and Agencies identify manpower and personnel assigned IT/IA functions, enter the required information into the appropriate databases, and maintain these databases as changes occur.	1	$12.5M Update: $13.125M
Recommendation 2: Direct the OASD (C3I) to work with the OUSD (A&T) and the OUSD (P&R), as part of the Inherently Governmental Working Group (IGWG), to revise IT function codes and develop definitions that more accurately reflect today's IT and IA activities.	3	No cost
Recommendation 3: Direct the OASD (C3I) to draft guidance for review by the Inherently Governmental Working Group to be used by the DoD Components to determine core IT and IA requirements to minimize the risk of losing mission capability.	4	No cost
Recommendation 4: Direct the OUSD (A&T) to consider the merits of developing and maintaining a database that shows contractor staff-years against major functions, especially IT and IA.	4	No cost
Recommendation 5: Direct the ODASD (MPP) to establish a steering group composed of OSD, Joint Staff, and each of the Services (including the Coast Guard) to focus on military IT personnel issues.	4	No cost
Recommendation 6: Direct the ODASD (CPP) to work with the ASD (C3I) to widely publicize OPM flexibilities available to address civilian IT recruiting and retention problems.	13	No cost
Recommendation 7: Direct the OASD (C3I) to require the staffs of the DoD CIOs at the GS-13 through the GS-15 levels to complete the DoD CIO Certificate Program or the Advanced Management Program at the IRMC.	5	See Recomm. 9
Recommendation 8: Direct the OUSD (P&R) and the OASD (C3I) to issue policy directing the Services/Agencies to implement a mandatory requirement that DoD CIOs, Deputy CIOs, and SESs and flag officers on the CIO staffs attend DoD-sponsored ITM executive sessions.	6	See Recomm. 9
Recommendation 9: Direct the OUSD (Comptroller) to provide resources (personnel and funding) to the IRMC to accommodate additional training requirements of the DoD ITM workforce.	11	$5.8M Update: No Change
Recommendation 10: Direct the OASD (C3I) to work with the Joint Staff and the ODASD (CPP) to develop an IT contemporary issues training module for the CAP-STONE and APEX training sessions.	7	No cost
Recommendation 11: Direct the OASD (C3I) to officially adopt NSTISSI Number 4009, National Information Systems Security (INFOSEC) Glossary, as the official IA Glossary. This requires the Defense-wide Information Assurance Program (DIAP) to formally coordinate an annex defining terminology not yet officially adopted by NSTISSI but used by the Department.	8	No cost
Recommendation 12: Direct the Joint Staff to review the defensive information operations requirements in the context of JV 2010 and translate these requirements into the Universal Joint Task List (UJTL) and the Joint Mission Essential Task List (JMETL).	20	No cost

Recommendation	Page	Cost
Recommendation 13: Direct the OASD (C3I) to officially adopt the NIST Special Publication 800-16, Information Technology Security Training Requirements: A Role- and Performance-Based Model, and the NSTISSIs as the minimum DoD IA training standards.	8	No cost
Recommendation 14: Direct the OUSD (P&R) and the OASD (C3I) to establish the requirement that the CINCs, Services, and Agencies establish mandatory training and/or certification programs for the five "critical" IA functions, using the NSTISSC training standards and the IPT-developed certification requirements as the minimum requirement. In support of this, DISA shall develop baseline IA training courses to meet the IA training requirements stipulated in the IPT certification documents. These courses can then be used by the Services and Agencies to meet the certification IA training requirement or enhanced by the Services and Agencies to meet their unique needs.	8	$10.465M Update: No Change
Recommendation 15: Direct the OASD (C3I) to establish the requirement that no person assigned to a "critical" IA function at the entry level may be granted privileged access until the required IA training is successfully completed.	9	No cost
Recommendation 16: Direct the OUSD (P&R) and the OASD (C3I) to establish the requirement that the CINCs, Services, and Agencies document these certification programs in full, and develop the capability to readily produce detailed answers about the status of certifications.	9	Unknown —should be included in Recomm. 18.
Recommendation 17: Direct the OUSD (P&R) and the OASD (C3I), in concert with the CINCs, Services, and Agencies, to coordinate biennial reviews of each certification and/or training program to ensure the currency and utility of the requirements.	9	No cost
Recommendation 18: Direct the OUSD (P&R) and the OASD (C3I) to develop and establish an Advanced Distributed Learning program, including a certification management system, for IA training and education at DISA or other appropriate location. The IA Advanced Distributed Learning effort will support implementation of an IA element within the Federal Center for Information Technology Excellence proposed under PDD 63.	9	$48.75M Update: $34.8M
Recommendation 19: Direct the OASD (C3I) to incorporate into the DODD 8500.xx, Information Assurance, the requirement for contractors assigned "critical" IA functions to meet the same or equivalent certification and training requirements as Department personnel. This recommendation requires that the OUSD (A&T) provide guidance to Contracting Officers to ensure these requirements are included in affected contracts.	18	Unknown cost — unable to determine at this time

THIS PAGE INTENTIONALLY LEFT BLANK

Appendix K.
Service/Agency Costs to Implement Recommendation

Table 4. Service/Agency Costs to Implement Recommendations

Service/ Agency	Cost by Recommendation				Total Cost by Service/Agency
	Recomm. 1 (See Section 1.1.1)	Recomm. 9 (See Section 1.1.5)	Recomm. 14 (See Section 1.2.2)	Recomm. 18 (See Section 1.2.3)	
JCS	No cost		$25K	No cost	$25K
Army	$3M		$1M	No cost	$4M
Navy	$5.5M		$1.5M	No cost	$7M
Air Force	$3M		$1M	No cost	$4M
Marine Corps	$75K		$0.5M	No cost	$575K
OSD	DMDC - $50K CPMS – Unknown Update: CPMS - $600K (est.)		No cost	Year 1 - $5M Years 2 –5 - $10M each Update: Year 1-5 - $6.96M	$45.05M Update: $35.45M
DIA	$400K		$750K	Years 1-5:750K each Update: $0M	$4.9M Update: $1.15M
NSA	$500K		$2.5M	No cost	$3M
DLA	No cost		$1.5M	No cost	$1.5M
WHS	No cost		No cost	No cost	No cost
DISA	No cost		$720K	No cost	$720K
NIMA	No cost		$720K	No cost	$720K
BMDO	No cost		$250K	No cost	$250K
IRMC		$5.8M (annually)			$5.8M
Total Cost by Recommendation	**$12.525M Update:$13.125M**	**$5.8M**	**$10.465M**	**$48.75M Update: $34.8M**	**$77.5M Update: $64.19M**

THIS PAGE INTENTIONALLY LEFT BLANK

Appendix L.
Schedule of Recommendations